(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 716 549**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **94 01888**

(51) Int Cl[6] : G 06 F 11/34, 17/60, G 07 F 7/08, G 06 K 19/067G 06 F 157:00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 18.02.94.

(30) **Priorité :**

(43) **Date de la mise à disposition du public de la demande :** 25.08.95 Bulletin 95/34.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *LA POSTE Exploitant Public* — FR, *SLIGOS Société Anonyme* — FR et *SG2 Société Anonyme* — FR.

(72) **Inventeur(s) :** Sabatier Guy — *Cabinet Ballot-Schmit*, Gross Jean-Louis — *Cabinet Ballot-Schmit* et Perl Alain — *Cabinet Ballot-Schmit*.

(73) **Titulaire(s) :**

(74) **Mandataire :** Cabinet Ballot-Schmit.

(54) Procédé de détection de fraude dans le paiement par carte à pré-paiement.

(57) L'invention concerne un procédé de détection de fraude dans le paiement par carte à pré-paiement dans lequel un ou plusieurs terminaux de paiement sont en liaison avec un organe central de collecte d'information, ces terminaux étant susceptibles de débiter des unités correspondant au nombre d'unités consommées dans chaque carte effectuant une transaction.

Selon l'invention on établit un modèle caractérisant les consommations pour chaque type de terminal de paiement; chaque terminal de paiement est apte à effectuer des mesures de consommation journalières comprenant:

- la détermination du volume d'unités consommées,
- la détermination du nombre de transactions effectuées,
- la détermination de l'écart- type pour la distribution des consommations; en fin de journée, chaque terminal de paiement est apte transmettre ces mesures à l'organe central; l'organe central les compare aux modèles établis et, en fonction de critères préétablis détecte des anomalies.

Application au paiement par porte-monnaie électronique.

FR 2 716 549 - A1

PROCEDE DE DETECTION DE FRAUDE DANS LE PAIEMENT PAR CARTE A PRE-PAIEMENT.

L'invention concerne un procédé de détection de fraude dans le paiement par carte à pré-paiement avec lesquelles on peut réaliser des transactions financières (débit - crédit) en échange de biens ou de services.

L'invention trouve une application privilégiée dans ce qu'il est convenu d'appeler le paiement électronique. Dans de telles transactions les cartes constituent des "porte-monnaie" électroniques.

En effet, de nombreux biens ou services peuvent être obtenus par paiement à partir de terminaux de distribution de biens de consommation ou de services et/ou de terminaux de paiement au moyen de cartes à pré-paiement dites "porte-monnaie" électroniques. De telles cartes comportent pour cela dans une mémoire de type EPROM ou EEPROM des "unités de consommation",au sens large du terme.

A chaque transaction effectuée par le titulaire d'une telle carte, des unités correspondant au montant de la transaction sont débitées en conséquence. Le terminal de paiement auprès duquel est réalisée la transaction est crédité du montant correspondant.

Les terminaux et les cartes sont généralement équipés de moyen permettant de réaliser des échanges en toute sécurité. Ces échanges ont pour objet notamment de réaliser une mise à jour des soldes respectifs à chaque transaction réalisée.

D'autre part les terminaux de paiement sont reliés de façon directe ou non à un organe central de collecte d'informations également appelé système émetteur.

Cet organe est appelé émetteur car c'est lui qui, via des matériels de rechargement spécifiques charge et fournit les cartes à des organismes autorisés ou à des utilisateurs.

Cet organe permet en outre périodiquement de recueillir toutes les tansactions opérées sur chaque terminal, les unes après les autres. Cette collecte permet en particulier de mettre à jour les comptes des commerçants ou fournisseurs de services possédant un terminal de paiement, en portant sur leur compte les différentes transactions enregistrées par leur terminal.

Dans toute la suite de la description on parlera de terminal de paiement pour définir tout système à paiement par carte à pré-paiement, qu'il s'agisse de publiphones, de distributeurs de billets de transport, d'automates de toutes sortes ou de terminaux placés chez des commerçants.

Il est clair que l'utilisation de "porte-monnaie" électroniques n'est possible que si certaines conditions sont remplies : la sécurité de l'échange porte-monnaie/terminal, terminal/organe central doit être totale, les cartes doivent être infalsifiables et enfin les faux porte-monnaie doivent être impossibles à fabriquer.

C'est pourquoi on a recours à la technologie des cartes à microcalculateur car elle emploie des composants spécialement conçus pour offrir un très haut niveau de sécurité. Ces composants sont constitués d'une puce "mono-chip" comprenant un microprocesseur avec ses programmes, ses mémoires et ses moyens d'entrée-sortie. Mémoires et moyens d'entrée-sortie sont sous le contrôle du microprocesseur et de son programme, lequel ne peut être modifié extérieurement.

Par ailleurs, la sécurité des échanges s'appuie sur des techniques classiques en sécurité informatique. Il s'agit de garantir l'intégrité et l'authenticité du message envoyé par la carte débitrice et le terminal créditeur et/ou entre le terminal et l'organe central. On peut citer à titre d'exemple la procédure décrite dans l'article de P. REMERY, J.C. PAILLES, F. LAY intitulé "le paiement électronique" publié dans la revue "L'écho des Recherches", n° 134; 4ème trimestre 1988, pages 15, 24.

On pourra également se reporter à la demande de brevet FR 91 00680 publiée sous le numéro 2 671 889 dans laquelle un perfectionnement à la procédure précédemment citée a été décrit. Ce perfectionnement consiste à utiliser des clés multiples (K1, K2...) et des clés diversifiées (Ka5, Kb3). La carte à débiter calcule un certificat à l'aide de la clé diversifiée (Ka5) que le terminal à créditer reconstitue.

De telle mesures de sécurité sont quasiment infaillibles. Toutefois elles ne permettent pas de se protéger contre des fraudes telles que le vol de lots de cartes en phase terminale de fabrication ou la fabrication de fausses "vraies" cartes.

La présente invention a pour objet un procédé de détection de fraude permettant de remédier à ces inconvénients.

Le degré supplémentaire de sécurité apporté par le procédé selon l'invention repose sur une approche inhabituelle dans ce domaine particulier du paiement par cartes.

En effet, le procédé repose sur une approche statistique des phénomènes de consommation des différents terminaux de paiement.

La présente invention a plus particulièrement pour objet un procédé de détection de fraude dans le paiement par carte à pré-paiement comportant des unités à consommer, dans lequel un ou plusieurs terminaux de paiement sont en liaison avec un organe central de collecte d'information, ces terminaux étant susceptibles de débiter des unités correspondant au nombre d'unités consommées dans chaque carte effectuant une transaction, principalement caractérisé en ce qu'il comprend les étapes suivantes:

a) établir un modèle caractérisant les consommations pour au moins chaque type de terminal de consommation,

b) chaque terminal de paiement est apte à effectuer des mesures de consommation sur des durées déterminées, comprenant:

- la détermination du volume d'unités consommées,
- la détermination du nombre de transactions effectuées,
- la détermination de l'écart type pour la distribution des consommations,

c) à la fin de chaque durée déterminée , chaque terminal de paiement est apte à transmettre ces mesures à l'organe central

d) l'organe central compare les mesures reçues des terminaux aux modèles établis pour ces terminaux et, en fonction de critères préétablis détecte des anomalies.

D'autres avantages et particularités de l'invention apparaîtront à la lecture de la description qui est faite à titre d'exemple non limitatif et en regard des dessins sur lesquels :

- la figure 1, représente le schéma de principe de l'invention,

- la figure 2, représente une courbe correspondant à un exemple de modèle préétabli,

- la figure 3, représente sous la forme d'un diagramme, les paramètres permettant de définir des critères de détection de fraude,

- la figure 4, représente un exemple de procédure d'échange entre une carte et un terminal de paiement.

La figure 1, illustre les différentes étapes mises en oeuvre pour chaque élément du système (CE,A,B) permettant selon l'invention de détecter des anomalies de consommation. Ces anomalies permettent notamment de déceler des cas de fraudes telles que le vol de carte en phase finale de fabrication ou la fabrication de fausses cartes "porte-monnaie" électronique.

Ainsi selon le procédé, on réalise au préalable différentes mesures soit auprès de chaque terminal soit auprès de chaque type différent de terminal implantés chez des commerçants ou fournisseurs de services dans une zone géographique bien définie.

Ces mesures consistent à relever périodiquement le montant de chaque transaction c'est à dire le nombre d'unités consommées à chaque transaction et le nombre de transaction sur une durée donnée.

A titre d'exemple ce relevé peut-être fait chaque jour pendant un mois.

On peut à partir de l'ensemble des points de mesure relevés déterminer une valeur médiane Tmd pour le montant des transactions et une valeur moyenne Tmy ainsi que l'écart-type Em pour la distribution du montant des transactions (consommations individuelles). On dispose ainsi de données permettant d'établir un modèle caractérisant chaque terminal.

Ces modèles de référence peuvent bien entendu être révisés et modifiés tout au long de la vie du système pour tenir compte des évolutions observées sur les mesures.

On a représenté sur la figure 2, une courbe représentant un exemple de modélisation obtenu pour un type de terminal donné.

L'abscisse représente le montant des transactions, l'ordonnée représente le nombre de transactions.

Les données des modèles de référence ainsi établis sont enregistrées dans l'organe central de collecte d'information CE.

Le procédé consiste en outre pour chaque terminal B à mesurer sur des périodes de durée déterminées :

- le volume d'unités consommées (T) (c'est à dire le chiffre d'affaire c'est à dire encore le montant global de toutes les transactions ou opérations)
- le nombre N de transactions effectuées

à déterminer l'écart-type E pour la distribution du montant des transactions (consommations individuelles) et à transmettre à la fin de chaque période de durée déterminée le volume d'unités consommées, le nombre de transactions et l'écart-type ainsi obtenus.

Le volume d'unités consommé est obtenu par comptage des unités consommées Ti lors d'une première transaction et incrémentatoin du compteur à chaque transaction opérée pendant la période considérée.

Le nombre N de transactions est également obtenu par incrémentation d'un compteur de transactions.

L'organe central qui reçoit ces informations de chaque terminal auquel il est relié peut alors procéder à des comparaisons avec les modèles de références préalablement enregistrés.

Ainsi cet organe va comparer le volume de consommation T reçu avec le volume de consommation Tm du modèle (qui correspond à la surface hachurée sur la figure 2).

La détection de fraude peut ensuite être faite en fonction d'un ou de plusieurs critères de sélection définis dans la suite.

Un premier critère consiste à vérifier que le montant moyen d'une transaction ne dépasse pas le montant maximal autorisé.

Pour cela, l'organe détermine le montant moyen d'une transaction soit la valeur T/N (T étant le montant total des consommations et N le nombre de transactions) et comparer ce montant au montant maximal pour une transaction autorisée (montant qui est bien connu puisqu'il correspond au montant moyen présumé donné par l'étude de comportement, c'est à dire par le modèle).

Le deuxième critère consiste ensuite, dans le cas ou le premier critère est rempli à vérifier que le volume de transaction T est compatible avec l'intervalle de confiance que l'on s'est fixé au préalable. Cet intervalle est défini, par exemple, par deux bornes Tmax et Tmin correspondant à une fourchette de tolérance de quelques pour cent autour de la valeur médiane du modèle.

L'organe vérifie aussi que l'écart-type E est compris dans l'intervalle de confiance sur l'écart-type que l'on s'est fixé. Cet intervalle est défini par deux bornes Emin et Emax correspondant à une fourchette de tolérance de quelques pour cent autour de la valeur E.

Ainsi c'est à partir d'un couple de données (volume de transactions - écart-type ou nombre de transactions - écart-type) que l'on définit selon un mode préféré de

réalisation un critère de sélection permettant de détecter des anomalies.

Lorsque les résultats de comparaison se situent dans la zone de confiance définie par les intervalles (Tmax, Tmin) et (Emax, Emin) aucune anomalie n'est détectée. En dehors de cette zone, les données se trouvent dans une première zone de suspicion (Tmax+d, Tmin-d) et (Emax+e, Emin-e) ou dans une zone de forte suspicion. Dans ces cas, et plus particulièrement dans le cas de forte suspicion on a détecté une anomalie dans les consommations par rapport au modèle. Un déplacement de la valeur médiane ou de la valeur moyenne par rapport aux valeur du modèle enregistré peut signifier qu'il y a eu fabrication de fausses cartes ou "clonage" de carte.

On peut alors décider d'entreprendre une remontée d'informations plus complète sur les consommations effectuées dans la période considérée, afin de connaître l'origine de cette anomalie.

Dans les réalisations pratiques effectuées, les informations de mesure qui remontent à l'organe central, sont transmises par les terminaux tous les jours en fin de journée par une procédure automatique classique. Chaque terminal ou chaque automate off-line possède à cette fin des moyens classiques aptes à établir une communication avec l'organe central à travers un réseau de transmission. (Transpac entre-autre).

Selon un autre aspect de l'invention, afin d'assurer la sécurité des échanges opérés entre les cartes des utilisateurs et les terminaux et entre les terminaux et l'organe central, on prévoit d'équiper ces différents éléments d'un module de sécurité connu sous l'appellation SAM. Un tel module permet d'authentifier

les messages par une procédure telle que décrite dans l'article cité dans le préambule de la description ou par la procédure à clé diversifiée que l'on rappelle ci-dessous et qui est illustrée sur la figure 4.

On choisit au préalable dix clés K1, K2,...,K10, ce nombre 10 étant naturellement arbitraire et ne limitant pas le principe de la procédure. Une carte A est repérée par une identité (a). Par une fonction de hachage de cette identité (a) et de chacune des clés K1, K2...,K10 on obtient dix clés diversifiées Ka1, Ka2,..., K10.

De la même manière, le terminal B muni de son module SAM étant repéré par une identité (b), on constitue dix clés diversifiées Kb1, Kb2,..., Kb10.

Par ailleurs, à l'identité (a) correspond, par une fonction u donnée, un rang dans l'ordre des clés. Dans l'exemple illustré u(a) est supposé égal à 3. Cela signifie que la carte A se voit affecter la clé K3.

De la même manière, l'identité (b) définit un rang u(b) qui, dans l'exemple illustré, est supposé égal à 5. Cela signifie que le terminal B se voit affecter la clé K5.

Pour travailler avec le module du terminal B, dont le rang de la clé est 5, la carte A est pourvue de la cinquième clé diversifiée propre à A soit Ka5.

Pour travailler avec la carte A, dont le rang de la clé est 3, le terminal B est pourvu de la troisième clé diversifiée propre à B, soit Kb3.

Les échanges illustrés sur cette figure 4, sont les mêmes que ceux établis entre le terminal et l'organe central. Ainsi la remontée journalières des données est faite en toute sécurité.

De manière plus générale, pour des transactions à effectuer avec d'autres terminaux que B, il faudrait

écrire dans la carte A d'autres clés diversifiées Ka1, Ka2,....soit dix clés au maximum.

De même, dans le module du terminal B, ou, pour travailler avec d'autres cartes que A, il faudrait prévoir d'autres clés diversifiées Kb1, Kb2... soit dix clés au maximum

Afin de réaliser un débit de A au profit de B, la procédure se déroule alors de la façon suivante :

- la carte B transmet à la carte A sa demande avec le montant Ti, l'identité (b), le nombre N;
- la carte A utilise la clé diversifiée Ka5 pour calculer le certificat C;
- la carte A transmet le certificat C à la carte B;
- à partir de l'identité (a) de A et de la clé K5 qu'elle possède, la carte B calcule Ka5 ce qui lui permet de décrypter le certificat C.

REVENDICATIONS

1. Procédé de détection de fraude dans le paiement par carte à pré-paiement comportant des unités à consommer, dans lequel un ou plusieurs terminaux de paiement sont en liaison avec un organe central de collecte d'information, ces terminaux étant susceptibles de débiter des unités correspondant au nombre d'unités consommées dans chaque carte effectuant une transaction, caractérisé en ce qu'il comprend les étapes suivantes:

a) établir un modèle caractérisant les consommations pour au moins chaque type de terminal de paiement,

b) chaque terminal de paiement est apte à effectuer des mesures de consommation sur des durées déterminées, comprenant:

- la détermination du volume d'unités consommées,
- la détermination du nombre de transactions effectuées,
- la détermination de l'écart-type pour la distribution des consommations,

c) à la fin de chaque durée déterminée , chaque terminal de paiement est apte à transmettre ces mesures à l'organe central,

d) l'organe central compare les mesures reçues des terminaux aux modèles établis pour ces terminaux et, en fonction de critères préétablis détecte des anomalies

2. Procédé de paiement selon la revendication 1, caractérisé en ce que la détermination du volume d'unités consommées est réalisée par comptage des unités consommées lors d'une première transaction et

incrémentation de ce comptage à chaque transaction réalisée sur toute la durée déterminée.

3. Procédé de paiement selon la revendication 1, caractérisé en ce que la détermination du nombre de transactions effectuées est réalisée par comptage d'une première transaction et incrémentation de ce comptage à chaque transaction réalisée sur toute la durée déterminée.

4. Procédé de paiement selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il consiste à comparer le volume de consommation reçu au volume maximal autorisé et à refuser la transaction si ce volume est supérieur à la valeur maximale.

5. Procédé de paiement selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il consiste à comparer le volume de consommation à la valeur du modèle dans une plage de tolérance.

6. Procédé de paiement selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il consiste à comparer l'écart-type à la valeur du modèle dans une plage de tolérance.

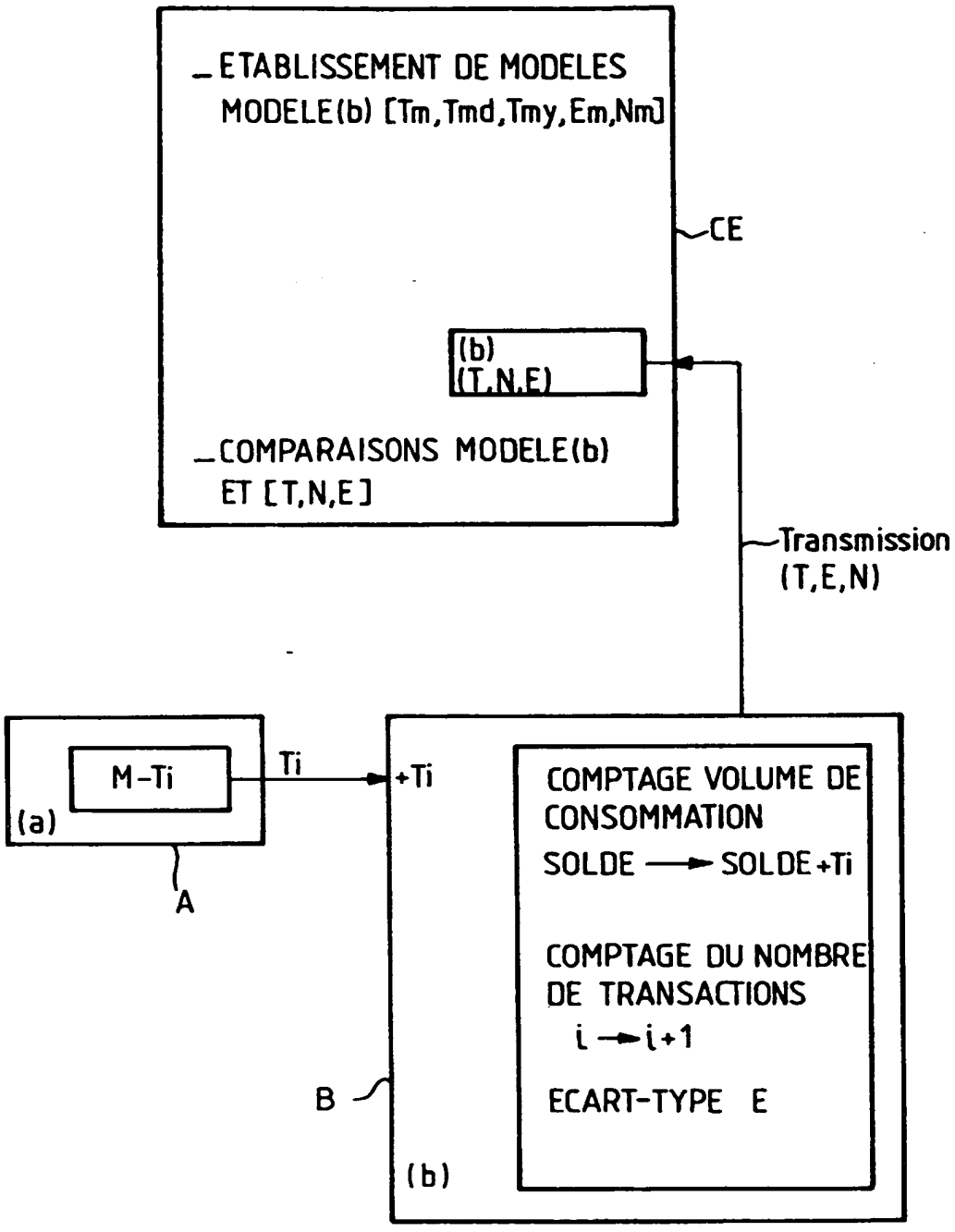
_ETABLISSEMENT DE MODELES
MODELE(b) [Tm,Tmd,Tmy,Em,Nm]
CE
(b)
(T,N,E)
_COMPARAISONS MODELE(b)
ET [T,N,E]
Transmission
(T,E,N)
M-Ti
Ti
+Ti
(a)
A
COMPTAGE VOLUME DE
CONSOMMATION
SOLDE → SOLDE+Ti
COMPTAGE DU NOMBRE
DE TRANSACTIONS
i → i+1
ECART-TYPE E
B
(b)

FIG_1

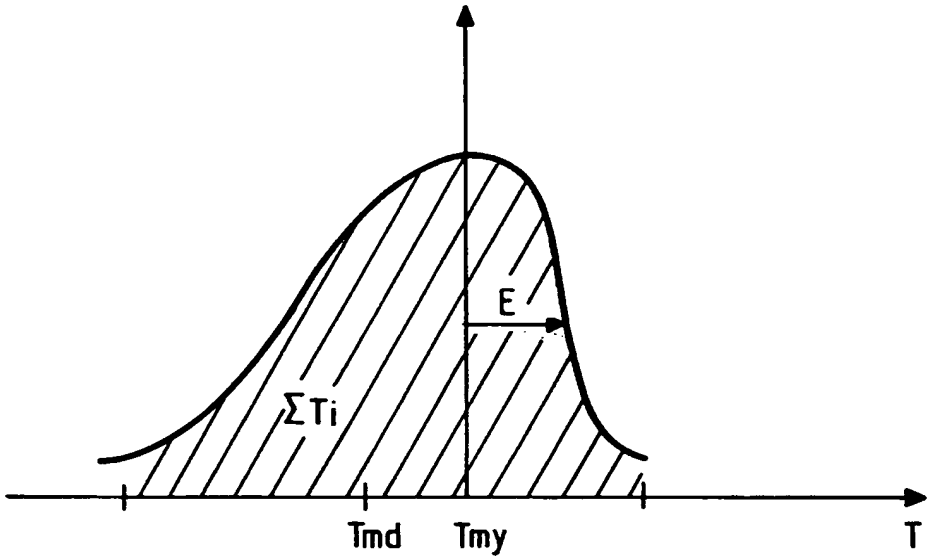
E
ΣTi
Tmd
Tmy
T

FIG_2

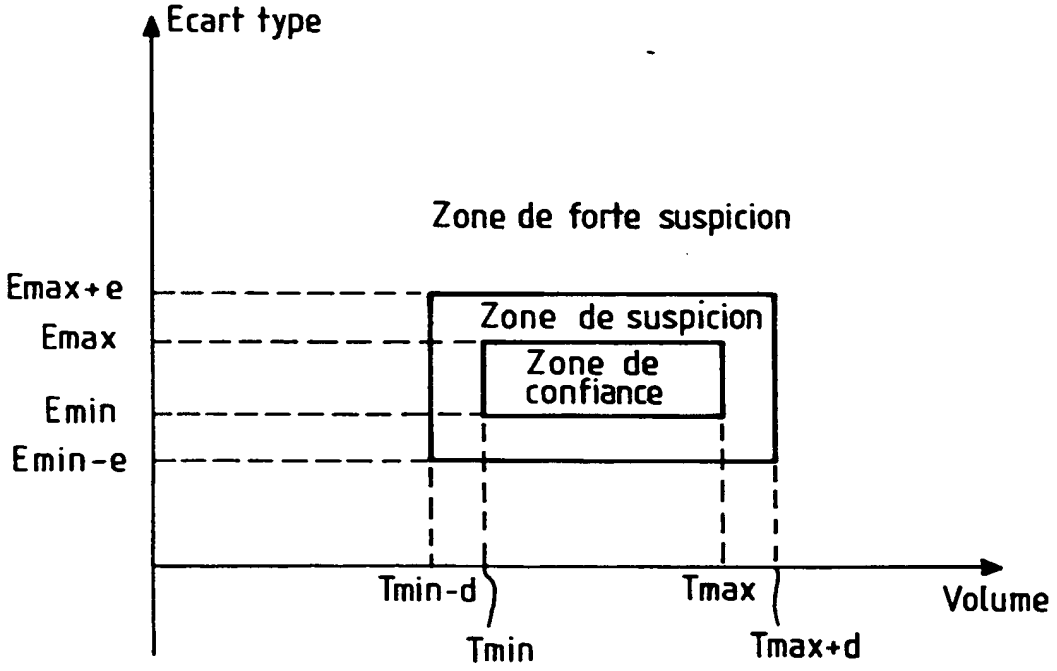
Ecart type
Zone de forte suspicion
Emax+e
Emax
Emin
Emin-e
Zone de suspicion
Zone de confiance
Tmin-d
Tmin
Tmax
Tmax+d
Volume

FIG_3

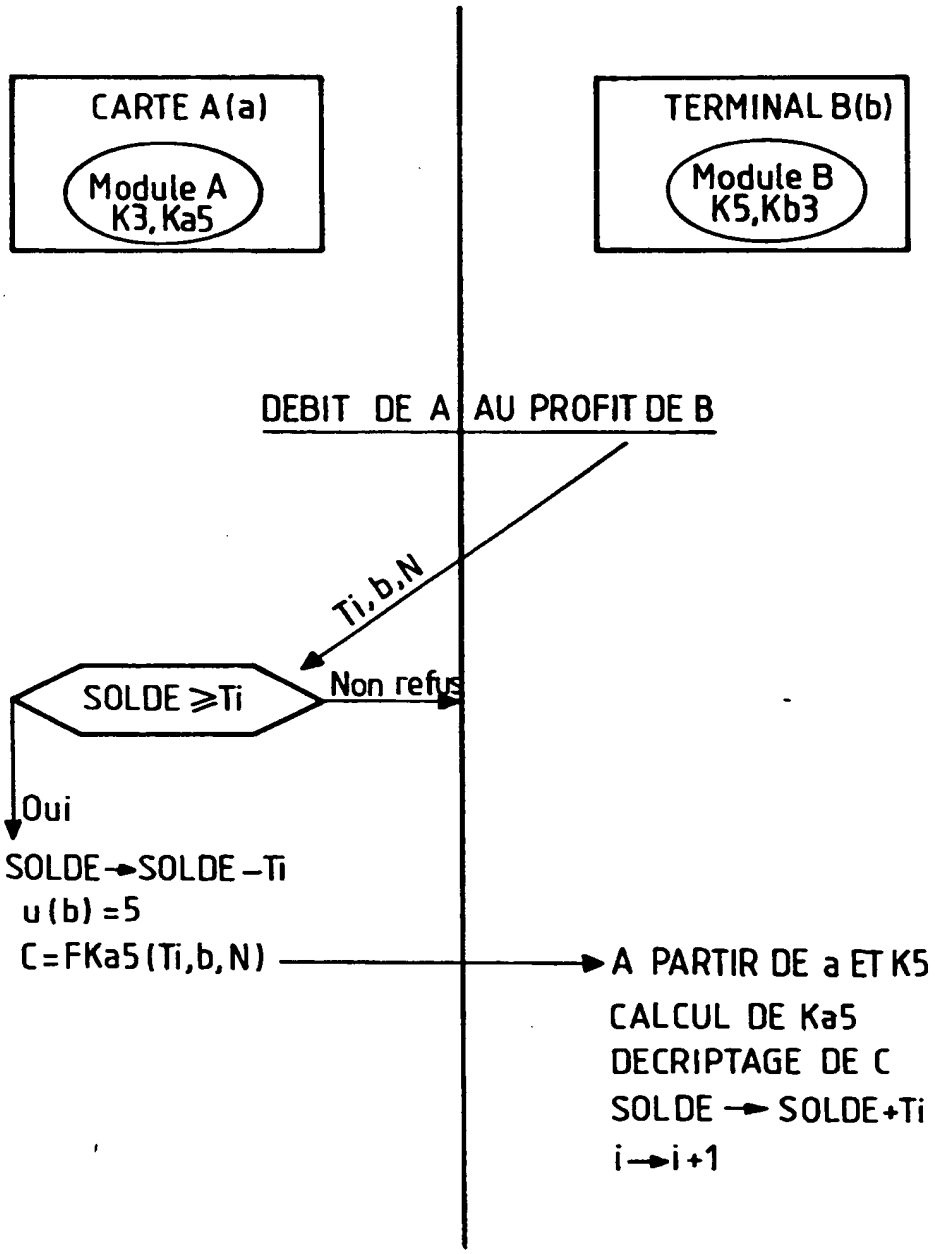
CARTE A(a)
Module A
K3, Ka5
TERMINAL B(b)
Module B
K5, Kb3
DEBIT DE A AU PROFIT DE B
Ti, b, N
SOLDE ≥ Ti
Non refus
Oui
SOLDE → SOLDE – Ti
u(b) = 5
C = FKa5 (Ti, b, N)
A PARTIR DE a ET K5
CALCUL DE Ka5
DECRIPTAGE DE C
SOLDE → SOLDE + Ti
i → i + 1

FIG_4

REPUBLIQUE FRANÇAISE

2716549

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 496226
FR 9401888

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
X A	EP-A-0 418 144 (ANDRÉ MICHAUD) * revendications; figures *	1 2-6
A	EP-A-0 004 497 (BERNARD SERRES ET.AL.) * abrégé; revendications 1-7; figures *	1-6
A	WO-A-89 06398 (ANDRÉ MICHAUD) * page 3, ligne 5 - page 4, ligne 44 * * page 7, ligne 25 - page 8, ligne 32 * * page 12, ligne 45 - page 14, ligne 38 * * page 17, ligne 27 - page 19, ligne 11; revendications 1-9; figures 6,7 *	1-4
A	EP-A-0 203 542 (SIEMENS A.G.) * abrégé; revendications 1-6 * * colonne 2, ligne 1 - colonne 3, ligne 33 *	1-6
A	EP-A-0 485 090 (VISA INTERNATIONAL SERVICE ASSOCIATION.) * colonne 7, ligne 1 - colonne 8, ligne 36; revendications 1-6 *	1-4
A	US-A-3 891 830 (ROBERT N. GOLDMAN) * abrégé; revendications 1-7 *	1
A	EP-A-0 200 343 (VISA INTERNATIONAL)	

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.5)

G07F
H04M

Date d'achèvement de la recherche: 8 Novembre 1994

Examinateur: Guivol, O

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)